Google

How to avoid COVID-19 online scams



Common types of scams



Falsely representing health organizations

Scammers posing as health authorities, such as the WHO or CDC, may offer cures, tests or other COVID-19 information.



Websites selling fraudulent products

Sites might offer hand sanitizer, face masks or other in-demand products that never arrive.



Posing as government sources

Some scams claim to issue updates and payments on behalf of the IRS or local government tax authority.



Fake nonprofit donation requests

Requests for COVID-19 donations to nonprofits, hospitals or other organizations should be checked carefully.



Fraudulent financial offers

Scammers may pose as banks, investors or debt collectors, with offers designed to steal financial information.

Tips to avoid common scams

Urgent message about COVID-19! Visit authoritative GovUSxba5@email.com ← : Know how scammers may websites directly reach you: through email, text for the latest updates Dear All, messages, automated calls, on COVID-19 and malicious websites This is a message from your government. In order to encourage more people to stay home we are Double check links offering a financial incentive of \$2000. and email addresses Never hand out personal To claim your incentive, please fill out before clicking or financial details your personal information here and verify your bank details at unless you're sure www.claim-1t-here.g0v. who you're talking to Donate directly through the If you would like to support the charity's website instead of National Coronavirus Relief Fund, you can also make a donation here. clicking a link sent to you

Paste portions of suspect messages into search engines to see if they've been reported



Add an extra layer of security to your accounts with 2-Step Verification or 2-factor authentication

Report it. If you see something suspicious, report it to justice.gov/coronavirus

For more information on how to avoid COVID-19 online scams visit: safety.google/securitytips-covid19